12-1-2005

Spyware Regulation: National Legislation Should Prompt Industry Self-Policing

Erica Pines

SPYWARE REGULATION: NATIONAL LEGISLATION SHOULD PROMPT INDUSTRY SELF-POLICING

I. INTRODUCTION

Millions of people around the world use the Internet every day.[1] Whether they send email, buy books, or trade stocks, users naively trust that what they do on their computers is their private business. How wrong they are! In recent years, advertising companies have discovered ways to send advertisements to consumers that directly target each individual's Internet habits.[2] To know which advertisements should be sent to whom, companies need to do a little sleuthing. Spyware, "software programs designed to infiltrate a personal computer to track the user's web activity without that person's knowledge or consent," does just that.[3] Spyware can change individual computer settings, track personal information numbers, store credit card numbers, and access all personal data stored on a computer's hard drive, thereby shredding away every bit of privacy personal computer users think they have.[4]

All of this is done at the consumer's expense for the sake of advertising companies, which then bombard personal computers with an incessant stream of unwanted "pop-up" advertisements.[5] There is a broad consensus that spyware must be stopped. It causes damage

---

1. Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 803 (2003).

2. *See* Ronald R. Urbach, *Adware/Spyware: An Update Regarding Pending Litigation and Legislation*, INTELL. PROP. & TECH. L.J., July 2004, at 12.

3. Rich Ehisen, *States Vie with Feds to Stop Spyware*, 12 ST. NET CAPITOL J. 25, ¶1 (June 21, 2004), *at* http://www.legislate.com/capj/capj.cgi?issue=20040621.

4. *Id.*, ¶3 *at* http://www.legislate.com/capj/capj.cgi?issue=20040621.

5. *See id.*, *at* http://www.legislate.com/capj/capj.cgi?issue=20040621; Urbach, *supra* note 2, at 12.

and invades personal privacy.[6] There is no consensus, however, as to how to stop it.

Both houses of Congress have spent more than a year producing various drafts of anti-spyware legislation.[7] Yet, these drafts remain in committee with much left undone.[8] Congress failed to exert a unified effort recognizing the importance of anti-spyware legislation. Instead, it put spyware on the back burner while it tackled more pressing issues.[9] That is until California, the leading state in technology and privacy legislation,[10] took the initiative.[11]

On September 28, 2004, California passed anti-spyware legislation to protect California citizens from the deceptive and malicious effects of spyware.[12] Called the California Consumer Protection Against Computer Spyware Act ("the California Act", or "the Act"), it prohibits anyone other than a computer's authorized user from knowingly causing computer software to be copied onto a computer for purposes prohibited by the Act.[13] Less than one week after the California Act passed, the United States House of Representatives passed *two* bills.[14] Thus, after ignoring the spyware

---

6. Ehisen, *supra* note 3.

7. U.S. House of Representatives Bill Tracking Report for H.R. 2929, 108th Cong., LEXIS 2003 Bill Tracking H.R. 2929; U.S. Senate Bill Tracking Report for S. 877, 108th Cong., LEXIS 2003 Bill Tracking S. 877.

8. U.S. House of Representatives Bill Tracking Report for H.R. 2929, 108th Cong., LEXIS 2003 Bill Tracking H.R. 2929; U.S. Senate Bill Tracking Report for S. 877, 108th Cong., LEXIS 2003 Bill Tracking S. 877.

9. *See* David McGuire, *House Approves Spyware Bills*, WASH. POST, Oct. 8, 2004, at E5.

10. *California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, INTERNET LAW & REGULATION (P&F), *at* http://internetlaw.pf.com/subscribers/html/NewNewsArticles.asp (Sept. 3, 2004).

11. *California Governor Signs Legislation Against 'Spyware'*, NAT'L J. TECH. DAILY, Sept. 29, 2004, *available at* 2004 WL 74921992.

12. *Id.*

13. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947 (Deering Supp. 2004). Purposes prohibited by the Act include, among others, deceptively modifying a user's homepage, default webproxy, or bookmarks; deceptively collecting keystrokes or viewing history; preventing removal of or disabling of software; intentionally misrepresenting that software will be uninstalled or disabled; or deceptively rendering security, anti-spyware, or anti-virus software inoperative. *Id.* § 22947.2 (a)–(e).

14. Ted Bridis, *Bill Imposes Prison Time Over 'Spyware'*, BELLEVILLERNEWSDEMOCRAT.COM, *at* www.belleville.com/mld/charlotte/news/breaking_news/9860032.html (Oct. 7, 2004).

problem for over a year, it appears that the California Act may have prompted the House to act swiftly to pass its own spyware legislation.

This Note contends that although the California Act attempts to end spyware and its negative effects, it may not be the proper solution. Foremost, because the Internet's lack of geographic boundaries raises murky legal questions regarding interstate commerce and the dormant Commerce Clause, the Act may be unconstitutional. Even if the California Act passes constitutional muster, issues of personal jurisdiction and enforceability surface when assessing the effect California legislation can have on a national, and even worldwide, problem. Further, the two House bills fall short of providing the serious protection consumers need.

Part II presents the serious problem of spyware, its mal-effects, and how it manages to find its way onto users' computers. Part III summarizes the California Act's language and provides a critique of the Act's benefits and shortcomings. Part IV analyzes the many serious legal questions the California Act raises. Part V questions whether the California Act attacks the spyware dilemma from the proper angle, and proposes that national legislation should provide individual victims with a right to directly sue technology companies that permit spyware distribution through their networks, systems, browsers, software applications, and hardware. This radical alternative addresses the pressing issue of spyware head on—in a way that existing and proposed legislation does not. The California Act, while an important and necessary step toward ending spyware abuses, is not a final solution. Given the importance of the privacy rights at stake, there must be a drastic adjustment to the way legislators address the spyware problem.

II. BACKGROUND OF THE SPYWARE DILEMMA

A. The Nature of Spyware

The term "spyware" refers to software programs that advertising companies install onto an individual's computer, often without the person's consent, that track and collect personal information about the individual, also without consent.[15] Spyware comes in various

15. Urbach, *supra* note 2, at 12.

forms. One type simply installs "adware," which bombards the individual's computer with countless "pop-up" advertisements.[16] Another type of spyware program tracks information such as personal online activities, passwords, and credit card numbers.[17] This information may then be sold to third-party adware companies that infiltrate computer systems with adware and "pop-up" advertisements specifically targeted to the user's Internet surfing habits.[18]

While adware programs are simply annoying, spyware programs that actually track users' online activities and collect personal data can be dangerous. For example, spyware can access and collect any personal data stored on a computer's hard drive, including credit card numbers, personal identification numbers, online banking identification numbers, passwords, home addresses, and phone numbers.[19] This is done through "keystroke logging," a method that records every key typed on a computer.[20]

Spyware can also change individual users' personal computer settings. These changes may include "homepage hijackings that change a browser's start-up home page, URL redirectors that forward [website] requests to different [websites], or programs that co-opt a computer's available processing resources or use the computer as an open relay for spam."[21] Spyware programs can even erase users' hard drives.[22]

B. How Spyware Infects Users' Computers

Spyware programs can be installed or downloaded onto users' computers in numerous ways. Users are most commonly infected when they intentionally download free file-sharing software or other programs from the Internet.[23] Often, spyware companies will pay Internet sites such as Kazaa, a music file-sharing site, to bundle their spyware software with music programs.[24] Before users can

16. *Id.*
17. Ehisen, *supra* note 3.
18. *Id.*
19. *Id.*
20. Michael Tonsing, *The Battle Against Spyware Is Just Beginning*, FED. LAW., June 2004, at 16, 16.
21. Urbach, *supra* note 2, at 12.
22. Ehisen, *supra* note 3.
23. *Id.*; Urbach, *supra* note 2, at 12.
24. Ehisen, *supra* note 3; Urbach, *supra* note 2, at 12.

download the programs they desire, they must install the spyware. Users do so unwittingly when they click on a box containing a lengthy licensing agreement and a button that says "I agree" or "I accept."[25] Within the box is the contract one "signs" in order to download the music, or whatever files they happen to be. Buried within that contract is a notice that the desired program contains spyware.[26] Once users click "I agree" to obtain the desired files, they are in essence agreeing to have spyware installed onto their computers.

Spyware programs also infiltrate computers through much more deceptive means. "Drive-by downloads" automatically install spyware onto computers without giving users the option to accept or decline the installation.[27] Spyware programs can also be encrypted in email attachments.[28] The most ruthless spyware infects users' computers the instant users visit particular websites.[29] Companies program these websites simply to attach spyware to visitors' browsers whose security preferences are set too low.[30] As if accessing personal files, logging individuals' Internet activity, and obtaining credit card numbers were not bad enough, "most spyware is deliberately designed to be nearly impossible to uninstall."[31] Spyware has stolen personal and crucial information from individuals. It has corrupted their computers. It has violated their privacy rights under the California Constitution.[32]

Often people do not even know they have spyware on their computers.[33] They go about their business, paying bills online and ordering prescriptions, without even realizing others are watching

25. Urbach, *supra* note 2, at 12.
26. Ehisen, *supra* note 3.
27. Urbach, *supra* note, 2 at 12.
28. *Id.*
29. *Id.*
30. Ehisen, *supra* note 3.
31. Tonsing, *supra* note 20, at 16. This means, despite how cautious or limited individuals are in their Internet use, each step taken is still being logged, and the cruel effects of spyware cannot be reversed without wiping out all data on users' computers. *See id.*
32. *Computer Spyware: Hearing on S.B. 1436 Before the Assemb. Comm. on Bus. and Professions*, 2003–2004 Sess. (Cal. Aug. 12, 2004) [hereinafter *Hearing on S.B. 1436*].
33. Tonsing, *supra* note 20, at 16.

their every move.[34] Can consumers and authorized computer users go anywhere in cyberspace without being watched? What does spyware do to the individual's sense of security and trust on the Internet?

III. THE CALIFORNIA ACT

A. The Language of the California Act

Recognizing the vulnerability of its citizens to relentless spyware programs, California passed legislation to protect online activity and personal information.[35] In February 2004,[36] California State Senator Kevin Murray introduced the first bill attempting to protect California consumers from the deceptive and malicious effects of spyware.[37] After many amendments and modifications, the Senate passed the California Act, also known as the California Consumer Protection Against Computer Spyware Act (Senate Bill 1436), on August 26, 2004.[38] Just over one month later, on September 29th, California Governor Schwarzenegger signed Murray's anti-spyware legislation into law, and the Act became effective on January 1, 2005.[39]

Often criticized for being too broad, the California Act states, "[a] person or entity that is not an authorized user . . . shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to . . . "perform a number of prohibited acts.[40] The Act defines "authorized user" as a person who owns, or who the owner authorizes to use, the com-

34. *Id.*

35. *Hearing on S.B. 1436*, *supra* note 32.

36. California Bill Tracking, S.B. 1436, LEXIS 2003 Bill Tracking S. 1436, http://www.statenet.com.

37. *California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, *supra* note 10.

38. California Bill Tracking, S.B. 1436, *supra* note 36 (bill codified at CAL. BUS. & PROF. CODE § 22947 (Deering Supp. 2004)).

39. *California Governor Signs Legislation Against 'Spyware'*, *supra* note 11; Thomas Claburn & George V. Hulme, *California Toughens Spyware Laws—Many Companies Already Comply by Offering Customers Opt-out Alternative*, INFO. WEEK, Oct. 11, 2004, at 26, 26.

40. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947.2 (Deering Supp. 2004).

puter.[41] "Consumer" refers to an individual who lives in California and who uses the computer in question for "personal, family, or household purposes."[42]

The California Act addresses spyware's most nefarious activities. The Act prohibits a person or entity from intentionally modifying any Internet browser or security settings on an authorized user's computer.[43] It also prohibits collecting personally identifiable information including names, credit or debit card numbers, passwords or personal identification numbers, social security numbers, account balances, user activity logs, or addresses through keystroke logging. One may not install software without the user's knowledge or consent, or install programs that extract data from the user's hard drive.[44] Further, software programs may not legally prevent authorized users from attempting to block the installation of or disabling of software.[45] Nor may a software distributor intentionally misrepresent that the software will be uninstalled or disabled according to the user's wishes when this is not in fact the case.[46] Moreover, the Act prohibits a person or entity from removing anti-virus software from an authorized user's computer.[47] Finally, the Act proscribes taking control over an authorized user's computer to gain access to information or to cause damage to the computer.[48] The California Act also lists legitimate software functions, which are not considered surreptitious spyware actions, to which the Act does not apply.[49]

Although the California Act does not specifically address enforcement, it may provide for a private right of action for consumers and Internet Service Providers to bring lawsuits seeking actual damages, liquidated damages of up to $1000 per violation, and attorneys' fees against purveyors of software.[50] The Business and

41. *Id.* § 22947.1.
42. *Id.*
43. *Id.* §§ 22947.1–22947.4.
44. *Id.*
45. *Id.* §§ 22947.2–22947.3.
46. *Id.* § 22947.2.
47. *Id.*
48. *Id.* §§ 22947.2–22947.3.
49. *Id.* § 22947.3.
50. *Computer Spyware: Hearing on S.B. 1436 Before the S.*, 2003–2004 Sess. (Cal. Aug. 19, 2004); Reed Freeman Jr., *Federal and State Governments*

Professions Code codifies the California Act as a civil statute with only civil, and not criminal, penalties.[51]

B. Evaluating the California Act

Competing interests between consumers and the technology industry illustrate the benefits and drawbacks of the California Act. Consumer advocates want anti-spyware laws that vigilantly protect consumers' privacy by setting forth a clear, comprehensive set of prohibited acts and remedies.[52] Adware providers and other technology companies, on the other hand, fear that overly broad anti-spyware legislation could hinder legitimate Internet business, technological advances, innovation, and competition.[53]

In the final days before the California Senate passed Murray's anti-spyware legislation, the Internet industry presented numerous amendments that it considered crucial to its support of the bill.[54] The industry primarily concerned itself with the breadth of the proposed legislation.[55] Companies feared that the Act would make many legitimate and necessary software functions unlawful, thus exposing them to frivolous litigation.[56] Murray accepted their amendments, hoping to create a stronger bill that Governor Schwarzenegger would be more likely to sign.[57]

Many corporations, including Time Warner, the American Electronics Association, TechNet, and Yahoo!, ultimately backed Murray's bill.[58] These companies felt that the amendments tightened up the language of the bill to focus upon "practices that are really

---

Turn Their Attention to Spyware and Adware, E-COMMERCE L. & STRATEGY, Aug. 30, 2004, at 1, 5; Verne Kopytoff, *Legislation Aims to Block Spyware; State, Federal Bills Seek to Ease Net Users' Growing Frustration*, S.F. CHRON., Oct. 4, 2004, at C1. How exactly the number of violations is to be calculated and the details of enforcement have yet to be articulated. Amendment to CAL. BUS. & PROF. CODE § 22947, LEXIS 2005 Bill Text CA S.B. 355.

51. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947 (Deering Supp. 2004).

52. Urbach, *supra* note 2, at 14.

53. *Id.*

54. *See Hearing on S.B. 1436*, *supra* note 32.

55. *Id.*

56. *Id.*

57. *See California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, *supra* note 10.

58. *Id.*

most associated with spyware and deceptive business practices, the things that people complain about."[59] Without the amendments, major software products such as Microsoft's Windows operating system, and web browsers like Internet Explorer and Netscape, would have fallen within the Act's definition of spyware.[60] Many businesses were concerned that legitimate practices such as online banking, security updates, or pornography blocking, would put them at serious risk of expensive and time-consuming litigation.[61] Because the amendments mitigated these concerns, key industry players supported the California Act.[62]

Privacy proponents, however, criticized the amended version as too weak.[63] They pushed for a notice and consent provision requiring every software program to provide a pop-up window indicating when the program was about to install spyware and providing the user with an opportunity to refuse the installation.[64] Privacy proponents adamantly supported this language because it would provide for informed, consensual decisions regarding computer and Internet security.[65]

At the last minute, however, Murray accepted amendments to the Act that removed the notice and consent requirement.[66] The acknowledged main reason for removing the language was that no individual user would knowingly provide the consent needed to download the spyware.[67] This would cause advertising companies responsible for "pop-up" advertisements to go out of business. Without spyware, programs would not be able to track users' Internet activities, and would thus be unable to provide specifically targeted "pop-up" advertisements.[68] Murray desperately needed industry support for his Act to pass, and he knew he would not receive it if the

---

59. *Id.*
60. Tonsing, *supra* note 20, at 17.
61. *See Hearing on S.B. 1436*, *supra* note 32.
62. *California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, *supra* note 10.
63. *Id.*
64. *Id.*
65. *See id.*
66. *See* Kopytoff, *supra* note 50; *California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, *supra* note 10.
67. *See Hearing on S.B. 1436*, *supra* note 32.
68. Interview with James Jenal, Counsel, O'Melveny & Myers, in Los Angeles, Cal. (Sept. 27, 2004) (on file with author).

notice and consent language remained.

Murray also articulated another reason for removing the notice and consent requirement. Requiring companies to design the pop-up windows to provide notice, which would ultimately cause them to lose business, would be too costly.[69] Many legitimate software programs that do not "spy" on users' every move would be required to provide pop-up windows explaining what was about to be downloaded onto a user's computer.[70] Legislators were worried that users would refuse consent to legitimate programs out of fear of downloading harmful ones.[71] This would interfere with legitimate business and impede technological advancement.[72] Some legitimate companies might take a business risk and choose not to provide notice in order to avoid costs, exposing themselves to the possibility of litigation to prove that they are not in fact spyware.[73] Notice and consent, so the argument went, would chill the Internet industry[74] and make consumers too paranoid to conduct business online.

Notwithstanding these industry concerns, privacy proponents such as the Privacy Rights Clearinghouse and the World Privacy Forum believe that the Act's language is too weak to provide effective protection for California consumers.[75] The legislation's goal was consumer protection, and removing the notice and consent language left consumers vulnerable.[76] According to Beth Givens, Executive Director of the Privacy Rights Clearinghouse, "California is [not] putting its best foot forward in enacting this bill into law."[77] Referring to the California Act, Pam Dixon of the World Privacy Forum stated, "it's better to have no legislation than legislation that doesn't protect consumers."[78] In her view, if Californians think they have taken measures to protect consumers, the state will move onto

69. *See Hearing on S.B. 1436*, *supra* note 32.
70. *Id.*
71. *See id.*
72. *See id.*
73. *See id.*
74. *Id.*
75. *California Spyware Bill Gets Industry OK, Awaits Governor's Signature; Groups Critical*, *supra* note 10.
76. *Id.*
77. *Id.*
78. *Id.*

other issues even though the measures are inadequate.[79]

There are some consumer protection advocates, however, who do feel that the Act is a step in the right direction. Michael Ross of the California Alliance for Consumer Protection believes that until there is national legislation, it is better to have some consumer protection than none at all.[80] Ross believes that even without the notice and consent requirement there will be a "dramatic change" in the way software companies do business because "these companies are now scared to death."[81] Thus, legislators must walk a fine line between frightening software programmers in order to end spyware and impeding the advancement of Internet technology.

Critics of the California Act are also concerned that the legislation only imposes civil penalties under the Business and Professions Code and not criminal sanctions.[82] The Act provides for a private right of action and liquidated damages of up to $1000 per violation.[83] Placing anti-spyware legislation in the Business and Professions Code, however, emphasizes business regulation over privacy rights. Some question whether a $1000 fine per violation constitutes a sufficient deterrent, or whether companies will simply factor the cost of violations into their profit calculations. Moreover, criminal penalties could be a more effective deterrent.

State legislators, however, may be less willing to criminalize spyware dissemination.[84] Massachusetts, New York, and New Jersey's proposals providing for criminalization of spyware activity have remained "bogged down in committee" (although not necessarily due to their criminal provisions).[85] California's Act, on the other hand, providing exclusively for civil penalties, became law. If criminal sanctions are in fact impeding anti-spyware legislation's passage, legislation imposing only civil sanctions may be better than none at all.

The question remains, however, whether a law such as the California Act is the most effective way to tackle spyware invasions.

---

79. *See id.*
80. *Id.*
81. *Id.*
82. *See generally* Ehisen, *supra* note 3 (discussing states imposing criminal sanctions and those only imposing civil penalties).
83. *See supra* note 50 and accompanying text.
84. *See* Ehisen, *supra* note 3.
85. *Id.*

Perhaps, given spyware's extreme intrusiveness, a "good start" is insufficient. In order for Internet commerce to function, consumers need to feel secure when typing in their credit card numbers to buy a book, a plane ticket, or even a car. A "good start" may leave consumers feeling violated and unprotected. This too may impede technological advancement.

IV. ANALYSIS OF THE LEGAL QUESTIONS IMPLICATED BY THE CALIFORNIA ACT

California's anti-spyware legislation effort is laudable. The state has taken steps to protect its consumers from fraud, invasion of privacy, and malicious acts on the Internet. Facially, the California Act appears to protect individual computer users and to help them regain trust in the security of Internet activities. The California Act raises serious legal concerns, however, which ultimately suggest a need for national legislation. Although the California Act aims to protect California consumers, it may be unconstitutional because it arguably regulates interstate commerce in violation of the dormant Commerce Clause.[86] Further, even if the law is constitutional, since spyware programs affect individual computer users throughout the world, it is questionable whether a California law could be effectively enforced against perpetrators outside California borders.[87] National legislation, on the other hand, can provide broader enforcement and a strong deterrent.

Currently there are federal laws that arguably regulate the same subject matter as the California Act including the Federal Trade Commission Act,[88] the Computer Fraud and Abuse Act,[89] and the Electronic Communications Privacy Act.[90] In October 2004, the United States House of Representatives passed two additional pieces of legislation to help implement these existing federal laws.[91] If ratified, this legislation could preempt the California Act.[92]

---

86. *See* discussion *infra* Part IV.A.

87. *See* discussion *infra* Part IV.B.

88. 15 U.S.C. § 41 (1991 & Supp. 2004).

89. 18 U.S.C. § 1030 (1992 & Supp. 2004).

90. *Id.* § 2510.

91. Bridis, *supra* note 14 (referring to the Internet Spyware Prevention Act (I-SPY Act) and Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)).

92. These pieces of legislation could trump the California Act with much

Unfortunately, none of this legislation attacks the root of the spyware problem—lack of an adequate enforcement mechanism. Thus, national legislation should provide victims with a private cause of action against technology leaders who permit spyware to travel through their networks, systems, browsers, software applications, and hardware. This is the most effective way to provide Internet consumers nationwide with protection and a sense of security.

A. The California Act May Violate the Dormant Commerce Clause

The Commerce Clause of the United States Constitution states, "[t]he Congress shall have Power . . . to regulate Commerce . . . among the several States . . . ."[93] Although this language constitutes an affirmative grant of power to Congress, the Supreme Court has also interpreted the Commerce Clause to act as a "dormant," or implicit, limitation on states' authority to enact laws that unduly burden interstate commerce.[94] In other words, the dormant Commerce Clause prevents states from enacting regulation in certain areas designated to Congress, even if Congress has not yet acted in that area.

The Supreme Court has established two tests for determining whether state legislation violates the dormant Commerce Clause.[95] The first test asks whether the law facially discriminates against interstate commerce.[96] The Supreme Court has held that state laws that regulate commerce occurring outside state borders, regardless of whether the commerce has effects within the state, have been found to offend the dormant Commerce Clause.[97] This is a strict scrutiny test,[98] meaning that the Court will uphold a law only if it is proven necessary to achieve a compelling state interest.[99] The law must be

---

stronger penalties.

93. U.S. CONST. art. I, § 8, cl. 3.

94. Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258, 262 (Cal. Ct. App. 2002) (citing Healy v. Beer Inst., Inc., 491 U.S. 324, 326 n.1 (1989)); Jack L. Goldsmith & Alan O. Skyes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 788 (2001).

95. *Ferguson*, 115 Cal. Rptr. 2d at 262.

96. *Id.*

97. *Healy*, 491 U.S. at 336 (citing Edgar v. MITE Corp., 457 U.S. 624, 642–43 (1982) (plurality opinion)).

98. *Ferguson*, 115 Cal. Rptr. 2d at 263.

99. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 529 (2001).

narrowly tailored, and there must be no less restrictive means the state can employ to achieve its goals.[100] The Court's list of activities that qualify as affecting interstate commerce is expansive, and "it is unlikely that any state law regulating the Internet would avoid dormant Commerce Clause scrutiny."[101]

If the law does not facially discriminate against interstate commerce, the Court applies a balancing test to determine whether the law imposes a burden on interstate commerce that is "clearly excessive in relation to the putative local benefits."[102] Under this less restrictive test, the law is "presumptively valid" unless the burden imposed on interstate commerce greatly outweighs the benefits of the regulation.[103] The Supreme Court has recognized that virtually every state law will in some way affect interstate commerce.[104] Thus, "where the [law] regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[105]

The Court has also held that the dormant Commerce Clause prohibits state laws that lead to inconsistent regulatory burdens.[106] This requirement does not mandate uniformity in state laws, but does attempt to protect out-of-state actors burdened by the state law who are unable to partake in the political process of the state that created the law at issue.[107]

1. Recent Application of the Strict Scrutiny Test

A survey of recent court decisions applying the strict scrutiny test to laws that allegedly regulate commerce occurring outside a state's borders indicates that courts will most likely find that the

100. *Id.*
101. Joseph Hameline & William Miles, *The Dormant Commerce Clause Meets the Internet*, B. B.J., Oct. 1997, at 8, 9.
102. *Ferguson*, 115 Cal. Rptr. 2d at 262 (quoting C & A Carbone, Inc. v. Clarkstown, 511 U.S. 383, 390 (1994)).
103. Hameline & Miles, *supra* note 101, at 20.
104. *Id.* at 22.
105. *Ferguson*, 115 Cal. Rptr. 2d at 263 (quoting Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970)).
106. Goldsmith & Skyes, *supra* note 94, at 789.
107. *Id.* at 795.

California Act violates the dormant Commerce Clause. The most recent California case to address the dormant Commerce Clause in the Internet context is *Ferguson v. Friendfinders, Inc.*,[108] a 2002 California Court of Appeal case. In *Ferguson*, the challenged California law regulated the conduct of persons or entities doing business in California who transmitted unsolicited email documents containing advertisements to California residents, from equipment located in California.[109] The law targeted only those doing business in California; it covered only messages sent from computers located in California, to California residents located in California.[110] Applying the strict scrutiny analysis from *Healy v. Beer Institute*,[111] the California Court of Appeal concluded that the law did not violate the dormant Commerce Clause.[112]

Healy established the principles for determining whether interstate effects of state regulations on commerce violate the dormant Commerce Clause.[113]

> [A] state [law] that directly regulates commerce occurring wholly outside the boundaries of the state violates the commerce clause.... [T]o determine whether a [law] impermissibly controls commerce outside the state, a court should evaluate the practical effect of the [law] by considering "the consequences of the [law] itself... [and] how the challenged [law] may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation."[114]

Applying these principles, the *Healy* Court determined that the law in question violated the dormant Commerce Clause because it had the effect of controlling beer prices in other states.[115]

The *Ferguson* court applied the *Healy* principles and reached the opposite conclusion, upholding the California law.[116] The *Ferguson*

108. 115 Cal. Rptr. 2d 258 (Cal. Ct. App. 2002).
109. *Id.* at 260.
110. *Id.*
111. 491 U.S. 324 (1989).
112. *Ferguson*, 115 Cal. Rptr. 2d at 263–64.
113. *Healy*, 491 U.S. at 331–43.
114. *Ferguson*, 115 Cal. Rptr. 2d at 264 (citing *Healy*, 491 U.S. at 336).
115. *Healy*, 491 U.S. at 338–40.
116. *Ferguson*, 115 Cal. Rptr. 2d at 264–66.

court reasoned that the law in question did not regulate commerce occurring wholly outside California because the law applied only to unsolicited email sent from a computer in California to a California resident.[117] The court also determined that the California law did not regulate the "Internet or Internet use per se,"[118] which could extend beyond the borders of California. The California law *only* regulated individuals and entities doing business in California who use equipment within California to send unsolicited email to California residents.[119] The court determined that a geographic location could be established for the equipment located within California, and the California residents who were receiving the unsolicited emails within California.[120] The court therefore decided that the argument that this law "functions in cyberspace" and is "wholly insensitive to geographic distinctions" has no basis.[121] Since the California law in *Ferguson* only had effects within the state of California, the court did not concern itself with other states passing similar, conflicting regulations.

2. Applying the Strict Scrutiny Test to the California Act

Unlike the *Ferguson* law, the California Act's language regarding the origin or cause of the harm is not state-specific. The Act states that, "[a] person or entity that is not an authorized user, . . . shall not, with actual knowledge . . . cause computer software to be copied onto the computer of a consumer in this state and use the software to do . . . " a number of prohibited acts.[122] The law does not target any actor based upon geographic location. It imposes liability upon offensive websites and spyware programmers located anywhere California has the capacity to exercise jurisdiction, and therefore discriminates against spyware programmers choosing to engage in interstate commerce.[123] The California Act thus directly regulates

117. *Id.*
118. *Id.* at 264.
119. *Id.*
120. *Id.*
121. *Id.* (citing Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997)).
122. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE §§ 22947.2, 22947.3 (Deering Supp. 2004).
123. *See Pataki*, 969 F. Supp. at 169–70 (finding a New York Internet regulation that imposed liability on anyone over whom the state could exercise

commerce occurring wholly outside the state, and thus violates the dormant Commerce Clause under *Healy*.

Moreover, while the *Ferguson* law did not regulate "Internet or Internet use per se,"[124] the California Act specifically regulates Internet use that extends beyond California's borders. The California Act does not target people or entities within a specific geographic location who commit a specific act, such as sending unsolicited email messages from California computers to California citizens, but rather targets installing spyware, a specific Internet activity.[125] The spyware installers' location when they cause harm to California consumers' computers is irrelevant. All that matters is that spyware committed one of the prohibited acts mentioned in the California Act. The Act holds the spyware culprit liable, which thereby affects interstate commerce.

In *American Libraries Association v. Pataki*,[126] a Second Circuit district court found that a law prohibiting use of a computer to disseminate obscene content to minors violated the dormant Commerce Clause because the law regulated conduct occurring wholly outside the state of New York.[127] The *Pataki* court emphasized that the nature of the Internet "makes it impossible to restrict the effects of the New York Act to conduct occurring within New York."[128] Further, the *Pataki* law applied to "*all Internet activity*," and not only to email distributors within New York who sent email to others located within New York.[129] The California Act parallels the law questioned in *Pataki* in that it applies to all spyware-related violations across the Internet, and it would be impossible to restrict the effects of prohibiting spyware activities to conduct that only occurs within California.

As a result, the California Act directly discriminates against out-of-state citizens, while indirectly benefiting its own citizens. The legislature passed the California Act to protect its own citizens from

---

jurisdiction to be unconstitutional in violation of the dormant Commerce Clause).

124. *Ferguson*, 115 Cal. Rptr. 2d at 264.

125. CAL. BUS. & PROF. CODE §§ 22947.2, 22947.3.

126. 969 F. Supp. 160 (S.D.N.Y. 1997).

127. *Id.* at 163.

128. *Id.* at 177.

129. *Ferguson*, 115 Cal. Rptr. 2d at 265 (citing Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 171 (S.D.N.Y. 1997)).

the mal-effects of spyware.[130] The Act, however, reaches beyond California's borders, ultimately forcing non-California citizens to comply with its provisions. The law in *Pataki* did not withstand scrutiny because "conduct that [might have been] legal in the state in which the user act[ed could] subject the user to prosecution in New York and thus subordinate the user's home state's policy . . . to New York's local concerns."[131] Similarly, under California's anti-spyware legislation, those living in California enjoy an advantage over those living outside of California. If all forty nine other states fail to enact anti-spyware legislation or enact legislation inconsistent with the California Act, in the absence of federal legislation, the California Act potentially subordinates each state's policies to California's. Forcing all citizens to comply with both California's legislation and that that of their own state, would arguably constitute discrimination in violation of interstate commerce because this would place a greater burden on those living outside of California, while benefiting only Californians.[132]

The California Act thus appears to fail the dormant Commerce Clause's strict scrutiny test by discriminating against out-of-state participants in interstate commerce for the benefit of California residents. Although protecting California consumers from malicious spyware constitutes a compelling state interest, the state did not narrowly tailor the Act to further this interest, and there are less restrictive means available to meet California's objectives. As emphasized by the *Ferguson* law, one way for the California Act to withstand strict scrutiny is by narrowly tailoring it to specific actors within California.[133] Broadening the Act to cover all Internet activity opens the door to direct dormant Commerce Clause violations that could have been avoided if the law had been narrowly tailored to impact only California residents.

---

130. CAL. BUS. & PROF. CODE §§ 22947.

131. *Pataki*, 969 F. Supp. at 177.

132. This is not to say, of course, that California is exempt from having to follow other states' legislation if it applies to California residents. However, this is not relevant to the issue of whether the law at hand violates the dormant Commerce Clause. The only concern is whether the law discriminates against interstate commerce, while benefiting residents within the state imposing the legislation.

133. *Ferguson*, 115 Cal. Rptr. 2d at 265.

3. Applying the Balancing Test to the California Act

In addition to the conclusion that the California Act fails the strict scrutiny test by regulating commerce occurring wholly outside California's boundaries in a discriminatory fashion, the California Act also likely fails the dormant Commerce Clause's balancing test. Under the dormant Commerce Clause analysis, if a law does not facially discriminate against out-of-state interests, it may nonetheless be invalid if its incidental burdens on interstate commerce are clearly excessive in relation to the local benefits.[134] Although California has a very strong interest in protecting its citizens from spyware, this interest is outweighed by the burdens the Act imposes upon other states.

California is justifiably trying to protect its consumers from the negative and deceptive ramifications of spyware programs.[135] Spyware invades individuals' privacy and spyware programmers are untrustworthy.[136] Computer users often have no idea that spyware programs are present. Further, once a user does begin experiencing computer problems and determines that spyware is the offender, "most spyware is deliberately designed to be nearly impossible to uninstall."[137] This results in heavy costs to consumers in terms of time and money. States clearly have a substantial interest in preventing the cost-shifting to consumers inherent in the distribution of many spyware programs.[138] States also have a legitimate interest in protecting consumers against the use of spyware to delete the contents of hard drives, steal credit card and personal identification numbers, install computer viruses, and manipulate computer settings.[139] When California passed the Act, there was no national anti-spyware legislation in place. The need to act to prevent spyware's harms at a time when the federal government is failing to do so is also arguably a legitimate state interest.

---

134. *Id.* at 262.

135. *See* Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947 (Deering Supp. 2004).

136. *See generally* Norian, *supra* note 1 (discussing the need to maintain online privacy in a society where the current state of consumer privacy is grossly inadequate).

137. Tonsing, *supra* note 20, at 16.

138. *See Ferguson*, 115 Cal. Rptr. 2d at 268 (citing State v. Heckel, 24 P.3d 404, 410 (Wash. 2001)).

139. *See id.*

The burdens the Act imposes on interstate commerce nonetheless outweigh its local benefits. First and foremost, upholding the California legislation could encourage other states to pass similar legislation, ultimately subjecting spyware activities to inconsistent regulations and raising a major dormant Commerce Clause concern.[140] This is not to say that states may never enact their own regulations. To the contrary, the dormant Commerce Clause is not triggered every time states promulgate different substantive regulations.[141] Permitting each state, however, to implement its own anti-spyware legislation could result in constitutional violation.

> [W]hat is a legitimate use of the Internet in an individual's home state may be considered a violation of state law elsewhere. Thus, an individual must not only comply with his forum [state's Internet regulations], but he must also be aware of any current law regarding regulation of the Internet throughout the country.[142]

Different regulations across the country could result in such high compliance costs that they would outweigh any plausible regulatory benefits.[143] For example, technology companies might cease to develop new products for fear of being sued for violating any one of the many inconsistent state spyware laws. Legitimate websites might shut down out of fear of litigation, thus limiting society's access to valuable information. In this way, inconsistent legislation could chill advancement of technology nationally.

It is also possible that multiple inconsistent state laws will render spyware legislation unenforceable. With such varied anti-spyware legislation, spyware programmers may decide to take a calculated risk that they would fall through the cracks created by state law inconsistencies. As a result, laws like the California Act would have accomplished nothing, and would send the message to spyware programmers that the country has no control over spyware. This could result in more, rather than less, spyware, wreaking greater havoc than ever before.

The *Pataki* court stated, "the Internet is one of those areas of

---

140. Goldsmith & Skyes, *supra* note 94, at 789–90.

141. *Id.* at 790, 806.

142. Spencer Kass, *Regulation and the Internet*, 26 S.U. L. REV. 93, 104 (1998).

143. Goldsmith & Skyes, *supra* note 94, at 806–07.

commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."[144] This reasoning is sensible. The severe burdens that the California Act may impose upon interstate commerce demonstrate that spyware regulation is an area best suited for national control.

Overall, in weighing the burdens imposed on interstate commerce against the dangers that could result from inconsistent state regulations, it is clear that state interests must yield to the greater need to protect interstate commerce. Further, the states' legitimate interests in enacting spyware legislation might in fact be better served at the federal level. Thus, the California Act clearly violates the dormant Commerce Clause under both the strict scrutiny and balancing tests.

B. The Enforceability of the California Act

Even if the California Act passes constitutional muster, it would be outrageously impractical to enforce. United States House Representative Zoe Lofgren, a Democrat from California, said spyware is "quickly becoming one of the biggest threats to consumers on the Internet."[145] She was referring not only to California, or even to the United States, but to the entire world. A state law only affects one state, while spyware is truly a global problem.[146] Enforcing a California state law prohibiting spyware activity originating from any geographic source would only provide California residents with redress. The California Act does not protect consumers in the other forty nine states, or the rest of the world, from spyware. This raises questions as to the Act's effectiveness in eradicating spyware nationally. Moreover, the California Act's enforceability rests on the assumption that a spyware programmer can be identified for suit, which is generally not the case.

As Internet technology has boomed in recent years, the courts have had to play catch up with the interpretation of laws designed to regulate cyberspace.[147] Adapting existing laws that regulate

144. Am. Libraries Ass'n v. Pataki, 969 F. Supp 160, 169 (S.D.N.Y. 1997).
145. Bridis, *supra* note 14.
146. *See* Ehisen, *supra* note 3.
147. *See* Urbach, *supra* note 2, at 14.

traditional media forms, such as newspapers and television stations, to issues that arise on the Internet may work in some instances, but not in others. For example, the Internet raises unique questions of personal jurisdiction.[148] Whether a court has personal jurisdiction over a particular defendant depends on the extent of the defendant's contacts with the state in which the court sits.[149] The defendant has "minimum contacts" with the state if 1) the defendant purposefully availed itself of the privileges of conducting activities in that state, thereby invoking the benefits and protections of the state's laws, and 2) the cause of action arose from, or is substantially related to, the purposeful actions within the state.[150]

Applying the minimum contacts test to the Internet context can be confusing. When a person posts a website, it is unclear which state's laws govern activities resulting from use of the website. The fact that the website might be accessed anywhere in the world could mean that a defendant website developer could be subject to personal jurisdiction everywhere.[151] In *Zippo Manufacturing Company v. Zippo.com, Inc.*,[152] the court placed commercial Internet activities on a spectrum. Where the website falls on this spectrum determines whether the court has personal jurisdiction.[153] At one end of the spectrum are "passive" websites that simply make information available to users.[154] "Passive" sites do not confer personal jurisdiction on out-of-state defendants.[155] At the other end of the spectrum are "active" websites, which clearly do business and enter "into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet."[156] "Active" websites *do* confer personal jurisdiction on out-of-state defendants.[157] "The middle ground is occupied by interactive websites where a user can exchange information with the

148. *See* Kass, *supra* note 141, at 93.
149. Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).
150. *See id.*
151. Arthur R. Miller, *The Emerging Law of the Internet*, 38 GA. L. REV. 991, 995 (2004).
152. 952 F. Supp. 1119 (W.D. Pa. 1997).
153. *Zippo*, 952 F. Supp. at 1124.
154. *Id.*
155. *Id.*
156. *Id.*
157. *Id.*

host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website."[158]

The *Zippo* test has never been applied to spyware. Spyware does not fall neatly into any of the *Zippo* categories. Spyware programs are not websites, though some spyware programs do automatically download themselves onto users' computers when users visit a particular website. For spyware to be "active" in the *Zippo* sense, some form of business activity or contractual transaction would have to occur. Neither of these requirements exists with respect to spyware's uninformed, nonconsensual installations. Yet, spyware does satisfy *Zippo*'s requirement that there be "knowing and repeated transmissions of computer files over the Internet,"[159] as spyware distributors are aware of their transmissions, even if they do not know exactly where the spyware will end up, and users are not aware of its presence.

Spyware programs may nonetheless be "active" by analogy, therefore subjecting spyware distributors to personal jurisdiction in every state where harm occurs. Although spyware programs are not websites and do not conduct business directly with individual users whose computers the programs infiltrate, websites often hire spyware programmers to collect personal information about users who visit their websites. Websites thus often conduct spyware activities in anticipation of contracts.

Along those same lines, spyware programmers consciously and intentionally access individual computers via the Internet for commercial purposes—to sell products for the companies that hire them. Spyware programmers know they are tapping into users' computers all over the world. Under the *Zippo* analysis, then, spyware programs are "active" because they knowingly cause harm to computers in anticipation, in furtherance, and in pursuit of commercial activity. By this reasoning, spyware programmers should be subject to personal jurisdiction wherever harm occurs as a result of their programs.

This analysis presents hope for haling the world's spyware programmers and offending websites into California courts under the

158. *Id.*
159. *Id.*

Act. The question remains, however, as to how effective a state law designed to serve its own citizens can be at addressing a problem of global proportions. Granted, the Act may make California citizens feel more secure, and one cannot blame the California Senate for choosing to protect its citizens. A state law, however, is not the most effective means for reducing harmful conduct related to spyware. Thus, national legislators have a duty to protect the entire nation's citizens by passing federal spyware legislation.

The Internet industry strongly supports a national solution to the spyware problem.[160] Corporations do not want to be bothered with conflicting state regulations they may be concurrently violating in the course of business. One "strong national law,"[161] instead of up to fifty inconsistent laws, would facilitate compliance.

C. Current House Bills Leave Much to be Desired

Current legislation and the above analysis assume that victims of malicious spyware can *identify* the website or spyware program that caused them harm. To the contrary, users often only understand that their computers are not functioning properly without knowing why. Further, some spyware functions invisibly, such that consumers see no sign of violations.[162] Perhaps most infuriating, users sometimes know something is wrong, and know that spyware is the culprit, but cannot identify which spyware program caused the harm, when it did so, or how. This inability to identify the perpetrator, or even the harm, poses a serious obstacle to seeking effective redress against spyware programmers, and constitutes a major flaw in the California Act.

The two House bills passed in October 2004 to end spyware activity share the same flaw. While national legislation is a major step in the right direction, as it eliminates the problem of multiple, inconsistent bills, the end goal must always be kept in mind—the legislation must protect consumers from unauthorized spyware on their computers.

The House first passed the Securely Protect Yourself Against

160. Ed Fletcher, *Closing the Door on Spyware: State and Federal Efforts Target Software that Quietly Tracks Where Broswers Go on the Internet*, SACRAMENTO BEE, Mar. 29, 2004, at A3.

161. *Id.*

162. *See supra* Part II.

Cyber Trespass Act ("SPY ACT") on October 5, 2004, less than a week after California signed the California Act into law.[163] The SPY ACT imposes civil penalties that are much harsher than those under the California Act.[164] The SPY ACT provides for fines ranging from $11,000 to $3,000,000.[165] These steep fines may increase compliance. Further, the bill contains a notice and consent requirement, similar to that removed from the California Act.[166] It requires programmers to notify computer users in "plain language" that the program about to be downloaded will collect and transmit information about the user to other sources.[167] At that point, the user must have a clear option to grant or deny permission for the transaction.[168]

On October 7, 2004, the House passed a second bill, called the Internet Spyware Prevention Act ("I SPY Act").[169] This bill gives the United States Attorney General $10,000,000 to "crack down on companies and others that secretly install spyware" in order to discourage the use of spyware.[170] Those who violate the I SPY Act could face criminal penalties of up to five years in jail.[171]

Each of these bills articulates that it preempts and supersedes any state law that expressly regulates "deceptive conduct with respect to computers."[172] Although these bills facially appear to be much stronger and more effective against spyware than the California Act, it may be that neither will be enacted in its current form. Only the House passed the bills, just days before Congress was supposed to go home and work on the presidential race and their

163. *Bill Imposes Hefty 'Spyware' Fines* (Oct. 5, 2005), *available at* http://www.glispa.net/index.tempnews1.html.

164. Securely Protect Yourself Against Cyber Trespass Act, H.R. 2929, 108th Cong. (2003).

165. *Id.*

166. *Id.*

167. *Id.*

168. *Id.*

169. Internet Spyware Prevention Act of 2004, H.R. 4661, 108th Cong. (2003).

170. *Id.*; Bridis, *supra* note 14.

171. Internet Spyware Prevention Act of 2004, H.R. 4661, 108th Cong. (2003); Bridis, *supra* note 14.

172. Internet Spyware Prevention Act of 2004, H.R. 4661, 108th Cong. (2003); Securely Protect Yourself Against Cyber Trespass Act, H.R. 2929, 108th Cong. (2003).

own campaigns.[173] Critics of the House bills claim that the issue is not ripe for discussion, as shown by the fact that the House presented two separate bills.[174] Critics further contend that "you don't just pass something because Congress has an artificial deadline of going home this Friday or Saturday."[175] Thus, these critics believe that the House passed the bills too hastily, that more time should have been taken on such a serious issue, and that both Houses should have passed a unified bill. Further complicating the issue, the Senate also has spyware legislation of its own in the works.[176]

Various obstacles, including time and differences between the House and Senate bills, may hinder passage of the House bills. This could ultimately delay an effective federal solution even longer. In any event, the federal bills would not be effective for "12 months after [passage] and would automatically expire after 2009."[177] The California Act, by comparison, became effective on January 1, 2005. Preemption does not, therefore, immediately threaten the California Act.

Further, just like the California Act, the House bills do not account for the difficulty of identifying violative spyware programmers and websites, which surreptitiously download spyware onto users' computers.

V. A RADICAL PROPOSAL

Determining who or what entity is responsible for spyware destruction on users' computers is the main concern yet to be effectively addressed by either the California Act or the two House bills. In theory, users should be able to go after the spyware programmers or websites causing the harm. However, since they are so hard to identify, it may be impossible to enforce a judgment against them. Spyware programs could therefore continue to function without ramifications under all of the proposed spyware acts. This article proposes that legislators address this concern by holding responsible those with the power to minimize spyware harms, namely those who permit spyware to run over their networks

173. McGuire, *supra* note 9.
174. *Id.*
175. *Id.*
176. *Id.*
177. *Bill Imposes Hefty 'Spyware' Fines*, *supra* note 162.

and operating systems, and those who allow spyware to go undetected in their web browsers, software applications, and hardware.

This solution focuses less on who is directly at fault for spyware, and more on arriving at a workable solution to the problem by shifting the costs of harm away from innocent users and toward those industry players who are in the best position to protect consumers from spyware. Entities such as Microsoft, Dell, Adelphia, and Verizon have the resources and ability to solve the spyware problem for consumers.

To remedy the spyware problem, the Internet industry should police itself. Major manufacturers of computing hardware, operating systems and software applications, web browsers, and the multitude of major Internet providers all profit from consumers using the Internet where users access websites and spyware programs that cause them harm. These corporations are in the best position to crack down on malicious spyware. Major players could, for example, build spyware blockers into their software, browsers, and connections. Just as these companies distribute and constantly update anti-virus programs, they can produce and distribute anti-spyware programs and constantly update them as spyware evolves. Major industry players have the resources and capability to prevent spyware from infecting our computers and poisoning our lives.

Currently, many Internet-related companies have created programs designed to block "pop-up" advertisements as well as programs that give consumers more control over what websites download onto their computers.[178] For instance, Internet Service Providers "have made pop-up blocking software a standard part of their services."[179] Additionally, Microsoft has developed a new service pack for Windows XP that will display a dialog box on computer users' screens whenever applications try to install themselves onto users' computers, and provide management tools to help disable those applications.[180] It is evident that these

178. Urbach, *supra* note 2, at 14–15.

179. *Id.* at 14. However, these pop-up blocking features are only effective against ads that are served by a website; they are ineffective against ads that are served by third-party applications that install adware or spyware programs onto individual users' computers. *Id.*

180. *Id.* at 14–15.

corporations have the capability to create programs that prevent spyware activities, yet nothing requires them to do so. As a result, there is haphazard and unreliable protection from the ones with the greatest potential for ending the spyware phenomenon. The possibility of exposure to liability for harm to consumers, however, would prod the industry into full gear, on a global basis.[181] Thus, placing liability on major Internet providers is the most effective way to protect computer users from spyware nationwide.

When the Internet began, the number and nature of Internet users was limited.[182] As a result, the protocol for designing computers and Internet controls presumed the existence of trusting relationships. Thus, the Internet did not require or develop many security or preventative measures. This is no longer true today. Many Internet users and service providers are not trustworthy, and consumers need more protection than what currently exists. If the goal of anti-spyware legislation is to end spyware maladies, going after the "little guys," the spyware programmers, will not achieve it. Instead, legislation should target the industry's deep pockets, those who profit from the status quo and who can and should be responsible for industry excesses.

A national bill allowing computer users harmed by spyware to directly sue major manufacturers of operating systems, application programs, hardware, and web browsers, as well as major Internet Service Providers, would provide victimized users with an *identifiable* defendant, from whom to seek redress.

A comparison can be drawn between liability for harm caused by spyware and harm caused by car accidents. Car owners may sue Ford or General Motors for product defects or malfunctions when a car is unsafe. A web browser or operating system that allows thousands of spyware programs to invade personal computers and harm users is similarly defective and unsafe. Just as society holds car manufacturers accountable for unsafe defects, we should hold the Internet industry accountable for harms caused by spyware. The Internet industry is permitting pernicious software programs to flow

181. To further ensure compliance, the legislature could consider providing tax write-offs to Internet-related companies for the money spent on developing the necessary technology, programs, and applications to provide national spyware protection.

182. Interview with James Jenal, *supra* note 68.

across their networks, through their equipment, and via their software applications, extracting private information from users' computers. Users should be able to collect damages from these actors for these harms. Granted, the harm to an individual from unsafe computers is more subtle than that caused to an individual from a car defect. Nevertheless, both industries must be held equally accountable for allowing detrimental, invasive, and malicious harm.

The California Act and the two House bills provide reliable language defining what Internet activities constitute spyware, and what conduct can be sanctioned. Yet, the bills share the same flaw: it is virtually impossible to find a proper defendant from whom consumers may seek adequate reparation. The proposed national bills will provide for uniform regulations, which will increase compliance and enforceability.[183] Legislation, however, allowing spyware victims to sue identifiable defendants for harm caused by spyware is the only way to create an incentive for those with the means to prevent spyware to do something to stop the harm. Therefore, legislation allowing Internet-related corporations to be held liable for spyware activities attacks the spyware issue head on, and is the only plausible way to meet legislators' goal of realistically protecting American Internet users from malicious and surreptitious spyware acts.

VI. CONCLUSION

The spyware problem requires a national solution.[184] Legislation that provides clear guidelines and attainable remedies for violations will encourage compliance out of fear of litigation. Allowing states to govern this arena will only produce inconsistent laws that will frustrate legitimate software companies while possibly permitting those who violate privacy rights to "fall through the cracks." Multiple inconsistent state laws could impose unrealistic compliance costs on legitimate Internet companies, which may stifle innovation and the Internet services our society requires. Meanwhile, spyware companies may thrive on the inconsistencies, and continue to engage in wrongful conduct, simply factoring the cost of violations into their profit calculations.

183. *See supra* Part IV.A.3.
184. *See* Urbach, *supra* note 2, at 15.

National legislation has the power to prevent deceptive spyware companies from infecting innocent users' computers while promoting innovation, legitimate business, and the proliferation of useful software programs. Even California State Senator Kevin Murray, the author of the California Act, stated, "[i]n the best of all possible worlds, the federal government can do a broader job of enforcing things . . . . I don't mind them preempting my bill, as long as they preempt me with a bill that does something that is just as strong and tough on behalf of the people."[185]

The inability to identify spyware programmers and websites inflicting harm on users has made current state and national legislation ineffective. Unlike the government, however, the computer industry has the resources and capability to regulate spyware. The industry should police its own excesses and federal legislation should provide a strong incentive to do so. National legislation allowing spyware victims to sue key industry players would provide consumers with an identifiable defendant from whom to seek effective redress. Industry leaders should either hold themselves accountable, or be held accountable for failing to prevent programs they know are malicious from traveling across their systems and networks into the equipment of hapless users. Thus, national legislation holding the Internet industry liable for surreptitious and deceptive spyware harms is the most effective way to prevent spyware from thriving anywhere within the United States and the world.

*Erica Pines**

185. Ehisen, *supra* note 3.

* J.D. Candidate, May 2006, Loyola Law School, Los Angeles; B.A. Mass Communications and Social Welfare, University of California, Berkeley, 2002. My gratitude goes out to the editors and staff of the *Loyola of Los Angeles Law Review* for all their tireless efforts. Special thanks to Professor James Jenal and Glenn Anaiscourt for their insight and direction. Above all, I thank my family and friends for all their support and encouragement.